JP920020222US1 02 222 RPS

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 １月２８日

出 願 番 号
Application Number: 特願２００３－０１８３０９

[ST. 10/C]: [ＪＰ２００３－０１８３０９]

出 願 人
Applicant(s): インターナショナル・ビジネス・マシーンズ・コーポレーション

２００３年１２月 ２日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０９９６０８

【書類名】　特許願

【整理番号】　JP9020222

【提出日】　平成15年 1月28日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 13/10

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　佐々木　健

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　伊藤　貴志子

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　美根　宏昭

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100108501

【弁理士】

【氏名又は名称】　上野　剛史

【復代理人】

【識別番号】　100104880

【弁理士】

【氏名又は名称】　古部　次郎

【選任した復代理人】

【識別番号】　100118201

【弁理士】

【氏名又は名称】　千田　武

【手数料の表示】

【予納台帳番号】　081504

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【包括委任状番号】　0207860

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　コンピュータシステム、コンピュータ装置、記憶装置のデータ保護方法、およびプログラム

【特許請求の範囲】

【請求項１】　ユーザの環境で動作するユーザ領域と、書き込み保護を必要とするアプリケーションが格納される隠蔽された領域とを有する記憶装置と、

前記記憶装置の前記隠蔽された領域に格納される前記アプリケーションを展開可能に構成され、擬似的なディスクスペースを提供するメモリと

を含むコンピュータシステム。

【請求項２】　前記記憶装置は、ＰＡＲＴＩＥＳ(Protected Area Run Time Interface Extension Services)の仕様、もしくはそれに準ずる規格仕様を満たし、前記隠蔽された領域はＰＡＲＴＩＥＳパーティションであることを特徴とする請求項１記載のコンピュータシステム。

【請求項３】　前記記憶装置は、ＢＩＯＳのサポートにより前記隠蔽された領域からのブートが実行されることを特徴とする請求項１記載のコンピュータシステム。

【請求項４】　データを保持する記憶装置を備えたコンピュータシステムであって、

前記記憶装置は、

ユーザの環境で動作する領域である第１のパーティションと、

前記第１のパーティションとは別の領域であって、書き込み保護を必要とするアプリケーションが格納される第２のパーティションとを含み、

前記第２のパーティションは、前記書き込み保護を必要とするアプリケーションの中から所定のアプリケーションが実行される際に、当該所定のアプリケーションを展開可能とする空き領域を有することを特徴とするコンピュータシステム。

【請求項５】　前記第２のパーティションは、ＰＡＲＴＩＥＳ(Protected Area Run Time Interface Extension Services)パーティションであることを特徴とする請求項４記載のコンピュータシステム。

【請求項６】　ユーザの環境で動作する第１の領域とユーザから隠蔽された領域である第２の領域とを形成可能な外部記憶装置を備えたコンピュータシステムであって、

前記第２の領域に格納されているアプリケーションの中から、所定のアプリケーションのブートをサポートするブートサポート手段と、

前記所定のアプリケーションに対する物主証明のための承認を行う承認手段と、

前記所定のアプリケーションが承認されたアプリケーションである場合に、所定のメモリ上の空き領域または前記第２の領域における空き領域に当該所定のアプリケーションをコピーして、擬似アプリケーションエリアを形成する擬似アプリケーションエリア形成手段と、を含み、

前記所定のアプリケーションへのアクセスは、前記擬似アプリケーションエリアに対して行われることを特徴とするコンピュータシステム。

【請求項７】　前記擬似アプリケーションエリア形成手段は、前記所定のアプリケーションのサイズを検出し、前記所定のメモリ上の空き領域または前記第２の領域の空き領域を調べて領域を確保した後、前記擬似アプリケーションエリアを形成することを特徴とする請求項６記載のコンピュータシステム。

【請求項８】　前記擬似アプリケーションエリア形成手段は、前記第２の領域に前記擬似アプリケーションエリアを形成する際に、前記所定のアプリケーションのサイズを検出して当該第２の領域のアンロックをＢＩＯＳに要求した後、当該擬似アプリケーションエリアを当該第２の領域に形成することを特徴とする請求項６記載のコンピュータシステム。

【請求項９】　ユーザの環境で動作するエリアであるユーザエリアと、ユーザから保護されたエリアであるホストプロテクティッドエリアとに区別されてデータを保持する記憶装置に対してアクセスするコンピュータ装置であって、

前記ホストプロテクティッドエリアからのブートをサポートすると共に、当該ホストプロテクティッドエリアにあるアプリケーションに対する物主証明のための承認をサポートするＢＩＯＳと、

前記ホストプロテクティッドエリアにある前記アプリケーションを他のメモリ

の空き領域または当該ホストプロテクティッドエリアの空き領域にコピーして擬似アプリケーションエリアを生成するアプリケーションアクセスモジュールと

を含むコンピュータ装置。

【請求項１０】　前記ＢＩＯＳは、秘密鍵の管理および/または前記ホストプロテクティッドエリアのアクセス管理を行うことを特徴とする請求項９記載のコンピュータ装置。

【請求項１１】　前記アプリケーションアクセスモジュールは、前記ホストプロテクティッドエリアにある前記アプリケーションがライトプロテクトされたものであるかどうかを判断すると共に、当該アプリケーションへのアクセスが行われる場合に、前記擬似アプリケーションエリアにアクセスすることを特徴とする請求項９記載のコンピュータ装置。

【請求項１２】　ユーザの環境で動作する第１のエリアとユーザから隠蔽された領域である第２のエリアとを有してデータを保持する記憶装置のデータ保護方法であって、

前記第２のエリアにある所定のアプリケーションをブートする際に、前記第２のエリアをアンロックするステップと、

アンロックされた前記第２のエリアから前記所定のアプリケーションを読み込むステップと、

アンロックされた前記第２のエリアをロックするステップと、

読み込まれた前記所定のアプリケーションを、他のメモリ上の空き領域に形成された擬似アプリケーションエリアにコピーするステップと、

前記擬似アプリケーションエリアから前記所定のアプリケーションをブートするための最初のコードを読み込むステップと

を含む記憶装置のデータ保護方法。

【請求項１３】　前記第２のエリアにある所定のアプリケーションが物主により承認されたアプリケーションか否かを判断するステップと、

前記所定のアプリケーションが承認されたアプリケーションである場合に、ライトプロテクトが必要かどうかを検出するステップと

を更に含む請求項１２記載の記憶装置のデータ保護方法。

【請求項１４】　ユーザの環境で動作する第１のエリアとユーザから隠蔽された領域である第２のエリアとを有してデータを保持する記憶装置のデータ保護方法であって、

前記第２のエリアにある承認されたアプリケーションをブートする際に、前記第２のエリアをアンロックするステップと、

アンロックされた前記第２のエリアから前記アプリケーションを読み込むステップと、

読み込まれた前記アプリケーションを、前記第２のエリアにおける空き領域に設けられた擬似アプリケーションエリアにコピーするステップと、

前記擬似アプリケーションエリアから前記アプリケーションをブートするための最初のコードを読み込むステップと

を含む記憶装置のデータ保護方法。

【請求項１５】　前記最初のコードを読み込むステップは、ディスクアクセスプログラムのアクセス範囲を、前記アプリケーションをコピーしたエリアに向けることにより、前記擬似アプリケーションエリアから当該最初のコードを読み込むことを特徴とする請求項１４記載の記憶装置のデータ保護方法。

【請求項１６】　ユーザの動作環境である第１のエリアとユーザから隠蔽された領域である第２のエリアとを有する記憶装置を備えたコンピュータに、

前記第２のエリアに対するアンロックを要求する機能と、

アンロックされた前記第２のエリアから、物主により承認され且つライトプロテクトが必要であるアプリケーションを読み込む機能と、

アンロックされた前記第２のエリアに対するロックを要求する機能と、

読み込まれた前記アプリケーションを、前記記憶装置とは異なるメモリ上の空き領域に設けられる擬似アプリケーションエリアにコピーする機能と

を実現させるプログラム。

【請求項１７】　前記コンピュータに、

前記擬似アプリケーションエリアから前記アプリケーションをブートする機能を更に実現させる請求項１６記載のプログラム。

【請求項１８】　ユーザの動作環境である第１のエリアとユーザから隠蔽さ

れた領域である第２のエリアとを有する記憶装置を備えたコンピュータに、

前記第２のエリアに対するアンロックを要求する機能と、

アンロックされた前記第２のエリアから、物主により承認され且つライトプロテクトが必要であるアプリケーションを読み込む機能と、

読み込まれた前記アプリケーションを、前記第２のエリアの空き領域に設けられる擬似アプリケーションエリアにコピーする機能と、

前記アプリケーションに対するアクセスを前記擬似アプリケーションエリアに向ける機能と

を実現させるプログラム。

【請求項１９】　前記アプリケーションに対するアクセスを前記擬似アプリケーションエリアに向ける機能は、当該アプリケーションに対するアクセステーブルのアドレスをコピー先のアドレスとする請求項１８記載のプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ハードディスクドライブ(ＨＤＤ)などの記憶装置を備えたコンピュータシステム等に係り、より詳しくは、所定のユーザ環境とユーザから隠蔽された領域とを有する記憶装置を備えたコンピュータシステム等に関する。

【０００２】

【従来の技術】

従来、業界標準規格であるＡＴＡ(AT Attachment)/ＡＴＡＰＩ(Advanced Technology Attachment Packet Interface)－５の仕様をサポートするハードディスクドライブ(ＨＤＤ：Hard Disk Drive)の機能を使用し、ＡＮＳＩ(American National Standards Institute)のスタンダードであるＰＡＲＴＩＥＳ(Protected Area Run Time Interface Extension Services)のアーキテクチャを用いて、ＨＤＤの中にユーザから隠蔽した領域、即ち、ユーザから自由にアクセスすることができない領域を作成することが可能である。

【０００３】

図７は、ＨＤＤにおけるＰＡＲＴＩＥＳの機能を説明するための図であり、Ｈ

ＤＤの領域を横に輪切りにしたイメージで表現している。ここでは、擬似的な最大領域である"Ｍａｘ"の値を定義し、通常のコマンドでは、この"Ｍａｘ"までが領域として与えられ、ＯＳは、"Ｓｔａｒｔ"から"Ｍａｘ"までを使用領域としている。この"Ｍａｘ"の値からＨＤＤにおける本当の最大領域である"Ｎａｔｉｖｅ Ｍａｘ"までがＰＡＲＴＩＥＳパーティション(PARTIES Partition)である。このＰＡＲＴＩＥＳパーティションにて規格が決まっている/もしくは定義されている"Boot Engineering Extension Record"には、ＰＡＲＴＩＥＳパーティションに入っている情報が格納されており、ここを参照することで、ＰＡＲＴＩＥＳパーティションに対する種々の機能を使用することができる。

【０００４】

このＰＡＲＴＩＥＳの仕様で想定されている使い方としては、通常、フロッピーディスクなどのリムーバルメディアからブートされるときにあてがわれるＡドライブを、ＰＡＲＴＩＥＳパーティションからブートするときにもあてがい、例えば、ＢＩＯＳ(Basic Input/Output System)のInterrupt４０というリムーバルメディアに対するＢＩＯＳコールを利用して、ＰＡＲＴＩＥＳパーティションに対するアクセスを行うサービスが存在する。即ち、ＰＡＲＴＩＥＳパーティションからブートして、Ａドライブが見え、通常の領域であるユーザパーティションをＣドライブとして見せるように構成している。これによって、ＰＡＲＴＩＥＳのエリアにＯＳのプリロードイメージを格納しておき、ここからのリカバリを可能としたり、ＢＩＯＳセットアップである、ハードウェアの設定、パスワードの設定、ブートシーケンスの記載等に必要な情報を、ＲＯＭに代わって格納し、例えば、グラフィカルなユーザインタフェースを用いたユーザによるセットアップ作業を可能としている。また、ブート(起動)プログラムを入れておき、ここからシステムの診断を行うこともＰＡＲＴＩＥＳの仕様として想定されている。

【０００５】

また、本件発明とは直接関係しないが、ハードディスクに対するデータ保護の従来技術として、入力されたパスフレーズをハッシュ関数によって処理し、ＨＤＤ内のデータを保護する技術がある(例えば、特許文献１参照。)。

【０００６】

【特許文献１】

特開２００１－３０６２６６号公報(第３頁、図１)

【０００７】

【発明が解決しようとする課題】

このような、ＡＴＡ/ＡＴＡＰＩ－５、およびＡＮＳＩ　ＰＡＲＴＩＥＳを用いて、書き込み保護したいＰＡＲＴＩＥＳのパーティションにおける書き込みを保護し、ＰＡＲＴＩＥＳパーティションに導入されているアプリケーションによるデータの変更を制限することが可能である。しかしながら、ＰＡＲＴＩＥＳパーティション上のアプリケーションを実行する場合、アプリケーション自身がＰＡＲＴＩＥＳのパーティションにあることから、読み込みや書き込みの制限を加えることは、現状の技術だけでは困難である。

【０００８】

ここで、ＰＡＲＴＩＥＳパーティション上のアプリケーションの内容は、物主(アプリケーションを作成して書き込んだオーナー)の証明のために、ハッシュ関数などのＢＩＯＳ内のプライベートキーを用いて承認が行われている。そのために、アプリケーションの内容が変更されると、即ち、ＰＡＲＴＩＥＳパーティション上のアプリケーションを実行して書き込みが行われてしまうと、承認されていない不正なアプリケーションとみなされ、アプリケーションの起動時にエラーとなってしまう。ＨＤＤでは、あるエリアだけを書き込み保護する機能は存在せず、ＰＡＲＴＩＥＳ用のパーティションを開発する場合に、書き込みの制限を意識して書き込み保護を実現する必要がある。

【０００９】

本発明は、以上のような技術的課題を解決するためになされたものであって、その目的とするところは、例えばＨＤＤ等の記憶装置において、ユーザから隠蔽された領域に格納されたデータに対する書き込み制限を実現することにある。

また他の目的は、例えば、ＨＤＤにおけるＰＡＲＴＩＥＳパーティション上のアプリケーション側でＰＡＲＴＩＥＳパーティション用にアプリケーションを変更、開発することなく、書き込みを制限することにある。

更に他の目的は、例えば、ＨＤＤにおけるＰＡＲＴＩＥＳパーティション上の

アプリケーションに対して、予期しない書き込みに対する対応を特別に行わなくとも、これらの書き込みに対する対応を可能とすることにある。

また更に他の目的は、ＰＡＲＴＩＥＳの仕様の利用範囲を拡張することにある。

【００１０】

【課題を解決するための手段】

かかる目的のもと、本発明が適用されるコンピュータシステムは、ＡＴＡ/ＡＴＡＰＩ－５、および、ＡＮＳＩ　ＰＡＲＴＩＥＳを用いて書き込み保護したいＰＡＲＴＩＥＳのパーティションの書き込みを保護し、ＰＡＲＴＩＥＳパーティションに導入されているアプリケーションによるデータの変更を制限している。即ち、本発明が適用されるコンピュータシステムは、例えば、ＰＡＲＴＩＥＳの仕様、もしくはそれに準ずる規格仕様を満たし、ユーザの環境で動作するユーザ領域と、書き込み保護を必要とするアプリケーションが格納される隠蔽された領域(例えば、ＰＡＲＴＩＥＳパーティション)とを有する記憶装置と、この記憶装置の隠蔽された領域に格納されるアプリケーションを展開可能に構成され、擬似的なディスクスペースを提供するメモリとを含む。ここで、この記憶装置は、ＢＩＯＳのサポートにより隠蔽された領域からのブートが実行されることを特徴とすることができる。

【００１１】

また、本発明は、データを保持する記憶装置を備えたコンピュータシステムであって、この記憶装置は、ユーザの環境で動作する領域である第１のパーティション(ユーザエリア)と、この第１のパーティションとは別の領域であって、書き込み保護を必要とするアプリケーションが格納される第２のパーティション(ＰＡＲＴＩＥＳパーティション、ホストプロテクティッドエリア)とを含み、この第２のパーティションは、書き込み保護を必要とするアプリケーションの中から所定のアプリケーションが実行される際に、この所定のアプリケーションを展開可能とする空き領域を有することを特徴とする。

【００１２】

一方、本発明は、ユーザの環境で動作する第１の領域とユーザから隠蔽された

領域である第２の領域とを形成可能な外部記憶装置を備えたコンピュータシステムであって、ブートサポート手段により、第２の領域に格納されているアプリケーションの中から、所定のアプリケーションのブートをサポートし、承認手段により、この所定のアプリケーションに対する物主証明のための承認を行い、この所定のアプリケーションが承認されたアプリケーションである場合に、擬似アプリケーションエリア形成手段により、所定のメモリ上の空き領域または前記第２の領域における空き領域にこの所定のアプリケーションをコピーして、擬似アプリケーションエリアを形成している。そして、この所定のアプリケーションへのアクセスは、擬似アプリケーションエリアに対して行われることを特徴とすることができる。

【００１３】

ここで、この擬似アプリケーションエリア形成手段は、所定のアプリケーションのサイズを検出し、所定のメモリ上の空き領域または第２の領域の空き領域を調べて領域を確保した後、擬似アプリケーションエリアを形成することを特徴としている。また、この擬似アプリケーションエリア形成手段は、第２の領域に擬似アプリケーションエリアを形成する際に、所定のアプリケーションのサイズを検出して第２の領域のアンロックをＢＩＯＳに要求した後、擬似アプリケーションエリアを第２の領域に形成することを特徴とすることができる。

【００１４】

他の観点から捉えると、本発明は、ユーザの環境で動作するエリアであるユーザエリア(User Area)と、ユーザから保護されたエリアであるホストプロテクティッドエリア(Host Protected Area)とに区別されてデータを保持するＨＤＤ等の記憶装置に対してアクセスするコンピュータ装置であって、ホストプロテクティッドエリアからのブートをサポートすると共に、このホストプロテクティッドエリアにあるアプリケーションに対する物主証明のための承認をサポートするＢＩＯＳ(Basic Input/Output System)と、ホストプロテクティッドエリアにあるアプリケーションを他のメモリの空き領域またはホストプロテクティッドエリアの空き領域にコピーして擬似アプリケーションエリアを生成するアプリケーションアクセスモジュールとを含む。

【００１５】

ここで、このＢＩＯＳは、秘密鍵の管理および/またはホストプロテクティッドエリアのアクセス管理を行うことを特徴とする。また、アプリケーションアクセスモジュールは、ホストプロテクティッドエリアにあるアプリケーションがライトプロテクトされたものであるかどうかを判断すると共に、このアプリケーションへのアクセスが行われる場合に、擬似アプリケーションエリアにアクセスすることを特徴とすることができる。

【００１６】

更に、本発明は、ユーザの環境で動作する第１のエリアとユーザから隠蔽された領域である第２のエリアとを有してデータを保持する記憶装置のデータ保護方法であって、第２のエリアにある所定のアプリケーションをブートする際に、この第２のエリアにある所定のアプリケーションが物主により承認されたアプリケーションか否かを判断するステップと、所定のアプリケーションが承認されたアプリケーションである場合にライトプロテクトが必要かどうかを検出するステップと、この第２のエリアをアンロックするステップと、アンロックされたこの第２のエリアから所定のアプリケーションを読み込むステップと、アンロックされた第２のエリアをロックするステップと、読み込まれた所定のアプリケーションを、他のメモリ上の空き領域に形成された擬似アプリケーションエリアにコピーするステップと、擬似アプリケーションエリアから所定のアプリケーションをブートするための最初のコードを読み込むステップとを含む。

【００１７】

他の観点から捉えると、本発明が適用される記憶装置のデータ保護方法は、第２のエリアにある承認されたアプリケーションをブートする際に、この第２のエリアをアンロックするステップと、アンロックされた第２のエリアからアプリケーションを読み込むステップと、読み込まれたアプリケーションを、第２のエリアにおける空き領域に設けられた擬似アプリケーションエリアにコピーするステップと、この擬似アプリケーションエリアからアプリケーションをブートするための最初のコードを読み込むステップとを含む。ここで、この最初のコードを読み込むステップは、ディスクアクセスプログラムのアクセス範囲を、アプリケー

ションをコピーしたエリアに向けることにより、擬似アプリケーションエリアから最初のコードを読み込むことを特徴とすれば、書き込み保護したいＰＡＲＴＩＥＳのパーティションの書き込み保護を実現できる点から好ましい。

【００１８】

ここで、本発明は、コンピュータに所定の機能を実現させるプログラムとして把握することができる。即ち、本発明が適用されるプログラムは、ユーザの動作環境である第１のエリアとユーザから隠蔽された領域である第２のエリアとを有する記憶装置を備えたコンピュータに、第２のエリアに対するアンロックを要求する機能と、アンロックされた第２のエリアから、物主により承認され且つライトプロテクトが必要であるアプリケーションを読み込む機能と、アンロックされた第２のエリアに対するロックを要求する機能と、読み込まれたアプリケーションを、記憶装置とは異なるメモリ上の空き領域に設けられる擬似アプリケーションエリアにコピーする機能と、擬似アプリケーションエリアからアプリケーションをブートする機能とを実現させる。

【００１９】

また、本発明が適用されるプログラムは、コンピュータに、第２のエリアに対するアンロックを要求する機能と、アンロックされた第２のエリアから、物主により承認され且つライトプロテクトが必要であるアプリケーションを読み込む機能と、読み込まれたアプリケーションを、第２のエリアの空き領域に設けられる擬似アプリケーションエリアにコピーする機能と、例えばアプリケーションに対するアクセステーブルのアドレスをコピー先のアドレスとして、アプリケーションに対するアクセスを擬似アプリケーションエリアに向ける機能とを実現させる。

【００２０】

尚、これらのプログラムとしては、コンピュータを顧客に対して提供する際に、装置の中にインストールされた状態にて提供される場合の他、コンピュータに実行させるプログラムをコンピュータが読取可能に記憶した記憶媒体にて提供する形態が考えられる。この記憶媒体としては、例えばＣＤ－ＲＯＭ媒体等が該当し、ＣＤ－ＲＯＭ読取装置等によってプログラムが読み取られて実行される。ま

た、これらのプログラムは、例えば、プログラム伝送装置によってネットワークを介して提供される形態がある。このプログラム伝送装置としては、例えば、ホスト側のサーバに設けられ、プログラムを格納するメモリと、ネットワークを介してプログラムを提供するプログラム伝送手段とを備えている。

【００２１】

【発明の実施の形態】

以下、添付図面に示す実施の形態に基づいて本発明を詳細に説明する。

[実施の形態１]

図１は、実施の形態１におけるコンピュータシステムの全体構成を示した図である。図１に示すコンピュータシステムは、大きくハードウェア１０とソフトウェア２０の構成要素に分けることができる。ここで、「システム」とは、複数の装置(機能)が論理的に集合した物をいい、各構成の装置(機能)が同一筐体中にあるか否かを問うものではない。従って、例えば、これらの構成要素が１つの装置にまとまって１つの取引対象となる場合もあり、また、特定の要素が別筐体として単体で扱われる場合もある。実施の形態２(後述)に示すコンピュータシステムも「システム」の考え方は同様である。

【００２２】

ハードウェア１０としては、ＯＳ(Operating System)/ユーザデータを保持するための不揮発性記憶装置であるＨＤＤ(Hard Disk Drive)１１、ＰＡＲＴＩＥＳ(Protected Area Run Time Interface Extension Services)パーティションをコピーするための記憶装置であるメモリ(Memory)１２を備えている。ＨＤＤ１１は、ＰＡＲＴＩＥＳの仕様を満たすために、ＡＴＡ(AT Attachment)/ＡＴＡＰＩ(Advanced Technology Attachment Packet Interface)－５の仕様をサポートしている。このＨＤＤ１１は、ユーザが自由にアクセスできる領域として、即ち、ユーザの環境で動作する領域(通常のパーティション)と、システムパーティションとして、ユーザから保護された、ユーザから隠蔽された領域であるＰＡＲＴＩＥＳパーティションとを備えている。また、メモリ１２は、ＲＡＭなどで構成され、擬似ＰＡＲＴＩＥＳアプリケーションエリア(後述)として使用される。

【００２３】

ソフトウェア２０としては、コンピュータシステムに接続されている各種デバイスを制御するＢＩＯＳ(Basic Input/Output System)２１、コンピュータシステムを提供する物主(システムベンダー：System Vendor)により提供された、ユーザから保護された領域(PARTIES Area)であるホストプロテクティッドエリア(Host Protected Area)２２、ユーザの環境で動作する領域であるユーザエリア(User Area)２４を有している。ホストプロテクティッドエリア２２には、ブート(Boot)可能なアプリケーションであり、システムベンダーにより提供されるサービスであるＰＡＲＴＩＥＳアプリケーション(PARTIES Application)２３が格納されている。

【００２４】

また、ソフトウェア２０には、ＰＡＲＴＩＥＳアプリケーション２３がライトプロテクト(Write Protect)されたものであるかどうかを判断するＰＡＲＴＩＥＳアプリケーションアクセスモジュール(PARTIES Application Access Module)２５、ＰＡＲＴＩＥＳアプリケーション２３をメモリ１２上にコピーしたワークエリアである擬似ＰＡＲＴＩＥＳアプリケーションエリア２６を有している。ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、上記の役割の他に、メモリ１２上の空き領域を調べて確保する役割、ＰＡＲＴＩＥＳアプリケーション２３をメモリ１２にコピーし、擬似ＰＡＲＴＩＥＳアプリケーションエリア２６を作る役割、ＰＡＲＴＩＥＳアプリケーション２３へのアクセスが行われる場合、擬似ＰＡＲＴＩＥＳアプリケーションエリア２６にアクセスする役割、を担っている。

【００２５】

ＢＩＯＳ２１は、ＰＡＲＴＩＥＳアプリケーション２３の仕様をサポートすると共に、ＰＡＲＴＩＥＳパーティションからのブートをサポートしている。また、ＰＡＲＴＩＥＳアプリケーション２３に対する、物主証明のための承認をサポートする機能の他、秘密鍵を管理する機能も備えている。更に、ホストプロテクティッドエリア２２のアクセス管理を実行する機能も備えている。

【００２６】

次に、ＰＡＲＴＩＥＳのパーティションにおける書き込み保護について説明す

る。

図２は、実施の形態１における書き込み保護方法を説明するための図である。ここでは、ブートが行われる場合、プロテクションされているセキュアなエリアであるＰＡＲＴＩＥＳパーティションを有するＨＤＤ１１に対して、ＢＩＯＳ２１から、ディスクアクセスプログラムであるＩＮＴ４０(Interrupt４０)に則ってディスクアクセスが実行される。ＨＤＤ１１の中にユーザから隠蔽した領域としてＰＡＲＴＩＥＳによって作成されるＰＡＲＴＩＥＳパーティションは、一旦、ユーザの環境からブートした後は、通常そのエリアについては触ることが出来ない。即ち、セキュアードなパーティションとして、ユーザの環境からはデータを壊されることがなく、データアクセスがなされることがなく、その結果、ウィルスの進入等を防ぐことも可能である。図２に示す例では、このＰＡＲＴＩＥＳパーティションに、ヘッダであるＢＥＥＲと、ＰＡＲＴＩＥＳアプリケーションとしてＰＳＡ０～ＰＳＡ５とが格納されている。

【００２７】

このＰＡＲＴＩＥＳパーティションには、システムベンダー(物主)により提供されるサービスであって、ユーザから保護されなければならないアプリケーションとして、

- Diagnostic Service
- OS Recovery Service
- Restore from backup Service
- Create diagnostic diskettes Service
- Download BIOS Service
- Download Drivers Service
- Update BIOS Service
- Administrator tools

等が格納される。

【００２８】

しかしながら、ＢＩＯＳ２１の例えばＩＮＴ４０によってＰＡＲＴＩＥＳパーティションにアクセスした場合、このＰＡＲＴＩＥＳパーティションのエリアに

あるアプリケーションを走らせてしまうと、ロックできずに、通常、書き込みが可能となってしまう。ＰＡＲＴＩＥＳパーティションのエリアにあるアプリケーションに対しては、ブート(Boot)に際して、ＢＩＯＳ２１の持つプライベートキーを用いてValidation(承認)が行われるが、ＰＡＲＴＩＥＳパーティション上のアプリケーションが変更されていると、Validationでエラーが起き、ブートすることができない。

【００２９】

そこで実施の形態１では、実行しようとするアプリケーションをＲＡＭ等のメモリ１２に全て展開し、擬似的なディスクスペースへのアクセスとして、ＰＡＲＴＩＥＳパーティションへの書き込み保護を実現する。図２に示す例では、ＰＳＡ３のアプリケーションをメモリ１２に一旦、展開している。このとき、例えば、メモリ１２の所定の領域に格納され、ディスクアクセスプログラムのアクセステーブルには、スタートとしてメモリ１２におけるＰＳＡ３´のスタートアドレス、エンドとしてメモリ１２におけるＰＳＡ３´のエンドアドレスが格納されている。これによって、リードもライトも、メモリ１２上のＰＳＡ３´となるように変更される。これによって、擬似的なディスクスペースにアクセスし、ＰＡＲＴＩＥＳパーティションへの書き込み保護を実現している。

【００３０】

図３は、実施の形態１におけるＰＡＲＴＩＥＳアプリケーションのブートの流れを示したフローチャートである。ＰＡＲＴＩＥＳアプリケーションのブートを実行するに際して(ステップ１０１)、まず、ＢＩＯＳ２１は、ホストプロテクティッドエリア２２をアンロックする(ステップ１０２)。次に、ＢＩＯＳ２１は、ホストプロテクティッドエリア２２のアクセス機能を用意する(ステップ１０３)。即ち、ディスクアクセスのルーチンを用意する。その後、ＢＩＯＳ２１は、ＰＡＲＴＩＥＳアプリケーション２３の承認(Validation)を行う。即ち、例えばＨａｓｈ値によって物主による承認を受ける(ステップ１０４)。そして、ＢＩＯＳ２１は、ホストプロテクティッドエリア２２をロックする(ステップ１０５)。ここで、ＢＩＯＳ２１では、承認されたアプリケーションか否かの判断がなされる(ステップ１０６)。承認されたアプリケーションではない場合には、ＢＩＯＳ２

１は、エラーを表示し、ブートを失敗させる(ステップ１０７)。ステップ１０６で承認されたアプリケーションである場合には、ステップ１０８に移行する。

【００３１】

ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、ＰＡＲＴＩＥＳアプリケーション２３のライトプロテクト(Write Protect)が必要かどうかを検出する(ステップ１０８)。そして、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、ＰＡＲＴＩＥＳアプリケーション２３のサイズ検出がなされる(ステップ１０９)。その後、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、メモリ１２の領域を確保し、擬似ＰＡＲＴＩＥＳアプリケーションエリア２６を作る(ステップ１１０)。そして、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、ＢＩＯＳ２１にホストプロテクティッドエリア２２のアンロックを要求し(ステップ１１１)、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、メモリ１２上に確保した擬似ＰＡＲＴＩＥＳアプリケーションエリア２６にＰＡＲＴＩＥＳアプリケーション２３をコピーする(ステップ１１２)。その後、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、ＢＩＯＳ２１にホストプロテクティッドエリア２２のロックを要求する(ステップ１１３)。これによって、ＰＡＲＴＩＥＳパーティション上にあるＰＡＲＴＩＥＳアプリケーション２３の書き込み保護が可能となる。

【００３２】

そして、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、擬似ＰＡＲＴＩＥＳアプリケーションエリア２６に対するアクセス機能(ディスクアクセスプログラム)を用意し、ＢＩＯＳ２１によって用意されたディスクアクセスプログラムと入れ替える(ステップ１１４)。その後、ＢＩＯＳ２１は、ブートのための最初のコードであるイニシャルプログラムローダを擬似ＰＡＲＴＩＥＳアプリケーションエリア２６から読み込み(ステップ１１５)、ＢＩＯＳ２１によるＰＡＲＴＩＥＳアプリケーション２３のブートが実行される(ステップ１１６)。

【００３３】

以上、詳述したように、本実施の形態では、ＨＤＤ１１における、実行しようとするアプリケーションを、全てＲＡＭ等のメモリ１２上に展開し、ＢＩＯＳ２

１によって、擬似的なディスクスペースへアクセスするように構成した。これによって、ＰＡＲＴＩＥＳパーティションへの書き込み保護を実現した状態にて、通常のアプリケーションをＰＡＲＴＩＥＳパーティション用のアプリケーションとして使用することが可能となる。

【００３４】

[実施の形態２]

実施の形態１では、ＰＡＲＴＩＥＳアプリケーション２３を、ＲＡＭ等のメモリ１２上に確保された擬似ＰＡＲＴＩＥＳアプリケーションエリア２６にコピーし、ＰＡＲＴＩＥＳパーティションへの書き込み保護を実現している。この実施の形態２では、ホストプロテクティッドエリア２２に確保された領域に擬似ＰＡＲＴＩＥＳアプリケーションエリア２６をコピーすることで、書き込み保護を実現している。尚、実施の形態１と同様の機能については、同様の符号を用い、ここではその詳細な説明を省略する。

【００３５】

図４は、実施の形態２におけるコンピュータシステムの全体構成を示した図である。ハードウェア１０の構成で、図１に示したメモリ１２をＰＡＲＴＩＥＳアプリケーション２３のコピーに用いていないことから、図４ではメモリ１２が除かれている。また、ソフトウェア２０の構成では、擬似ＰＡＲＴＩＥＳアプリケーションエリア２６をホストプロテクティッドエリア２２の空き領域にコピーしている点が異なる。かかる構成の違いによって、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５の役割として、図１にて説明した、ＰＡＲＴＩＥＳアプリケーション２３をメモリ１２にコピーし、擬似ＰＡＲＴＩＥＳアプリケーションエリア２６を作る役割の代わりに、ＰＡＲＴＩＥＳアプリケーション２３をホストプロテクティッドエリア２２の空き領域にコピーし、擬似ＰＡＲＴＩＥＳアプリケーションエリア２６を作る役割を担っている。

【００３６】

次に、ＰＡＲＴＩＥＳのパーティションにおける書き込み保護について説明する。

図５は、実施の形態２における書き込み保護方法を説明するための図である。

ここでは、ブートが行われる場合、プロテクションされているセキュアなエリアであるＰＡＲＴＩＥＳパーティションを有するＨＤＤ１１に対して、ＢＩＯＳ２１からＩＮＴ４０(Interrupt４０)に則ってディスクアクセスが実行される。図２に示す例と同様に、このＰＡＲＴＩＥＳパーティションに、ヘッダであるＢＥＲと、ＰＡＲＴＩＥＳアプリケーションとしてＰＳＡ０～ＰＳＡ５とが格納されている。このＰＡＲＴＩＥＳパーティションには、アプリケーションに使用している領域とともに、アプリケーションに使用していない領域(空き領域)がある。

【００３７】

実施の形態２では、このアプリケーションに使用していない領域を利用して、そこに実行しようとするアプリケーションを全てコピーし、このコピー部分に対してＩＮＴ４０によってアクセスする。図５に示す例では、アプリケーションのＰＳＡ３を書き込み保護を必要としない別のＰＡＲＴＩＥＳパーティションにコピーし(ＰＳＡ３´)、ディスクアクセスプログラムのアクセステーブルを変更して、ディスクアクセスプログラムのアクセス範囲をコピーしたエリアに向けるように構成し、このコピーしたエリアに対して、リードやライトを実行するようにした。即ち、ディスクアクセスプログラムのアクセステーブルには、スタートとしてホストプロテクティッドエリア２２におけるＰＳＡ３´のスタートアドレス、エンドとしてホストプロテクティッドエリア２２におけるＰＳＡ３´のエンドアドレスが格納されている。これによって、リードもライトも、ホストプロテクティッドエリア２２の空き領域に形成された擬似ＰＡＲＴＩＥＳアプリケーションエリア２６のＰＳＡ３´となるように変更される。これによって、擬似的なディスクスペースにアクセスし、オリジナルのＰＳＡ３の書き込みを制限すること、即ち、ＰＡＲＴＩＥＳパーティションへの書き込み保護を実現している。

【００３８】

図６は、実施の形態２におけるＰＡＲＴＩＥＳアプリケーションのブートの流れを示したフローチャートである。ＰＡＲＴＩＥＳアプリケーションのブートを実行するに際して(ステップ２０１)、まず、ＢＩＯＳ２１は、ホストプロテクティッドエリア２２をアンロックし(ステップ２０２)、ＢＩＯＳ２１は、ホストプ

ロテクティッドエリア２２のアクセス機能(ディスクアクセスプログラム)を用意する(ステップ２０３)。次に、ＢＩＯＳ２１は、ＰＡＲＴＩＥＳアプリケーション２３の承認(Validation)を行う。即ち、物主による承認(例えばＨａｓｈ値による承認)を受ける(ステップ２０４)。そして、ＢＩＯＳ２１は、ホストプロテクティッドエリア２２をロックする(ステップ２０５)。ここで、ＢＩＯＳ２１では、承認されたアプリケーションか否かの判断がなされる(ステップ２０６)。承認されたアプリケーションではない場合には、ＢＩＯＳ２１は、エラーを表示し、ブートを失敗させる(ステップ２０７)。ステップ２０６で承認されたアプリケーションである場合には、ステップ２０８に移行する。

【００３９】

ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、ＰＡＲＴＩＥＳアプリケーション２３のライトプロテクト(Write Protect)が必要かどうかを検出する(ステップ２０８)。次に、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５では、ＰＡＲＴＩＥＳアプリケーション２３のサイズ検出がなされる(ステップ２０９)。ここで、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、ＢＩＯＳ２１にホストプロテクティッドエリア２２のアンロックを要求する(ステップ２１０)。その後、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、ホストプロテクティッドエリア２２の空き領域に擬似ＰＡＲＴＩＥＳアプリケーションエリア２６を作る(ステップ２１１)。

【００４０】

次に、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、ＰＡＲＴＩＥＳアプリケーション２３を読み込み(ステップ２１２)、ホストプロテクティッドエリア２２に確保された擬似ＰＡＲＴＩＥＳアプリケーションエリア２６に、このＰＡＲＴＩＥＳアプリケーション２３をコピーする(ステップ２１３)。そして、ＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５は、ホストプロテクティッドエリア２２にコピーされた擬似ＰＡＲＴＩＥＳアプリケーションエリア２６に対するアクセス機能(ディスクアクセスプログラム)を用意し、ＢＩＯＳ２１によって用意されたディスクアクセスプログラムと入れ替える(ステップ２１４)。その後、ＢＩＯＳ２１は、ブートのための最初のコードであるイニシ

ャルプログラムローダを擬似ＰＡＲＴＩＥＳアプリケーションエリア２６から読み込み(ステップ２１５)、ＢＩＯＳ２１によるＰＡＲＴＩＥＳアプリケーション２３のブートが実行される(ステップ２１６)。

【００４１】

このように、実施の形態２では、ＰＡＲＴＩＥＳパーティションに導入されているアプリケーション(ＰＡＲＴＩＥＳアプリケーション２３)を実行する場合に、このアプリケーションの導入されているＰＡＲＴＩＥＳパーティションを、一度、書き込み保護を必要としない別のＰＡＲＴＩＥＳパーティションにコピーするように構成した。そして、元の領域に対するアクセスを、コピーした領域に対する領域に対するアクセスとなるように変更した。より具体的には、図５に示すように、アプリケーションに対するアクセステーブルのアドレスを、擬似ＰＡＲＴＩＥＳアプリケーションエリア２６のアドレスをコピー先のアドレスとなるように変更した。これによって、元の領域に対するアクセスを無くすことができ、書き込み保護を行いたいＰＡＲＴＩＥＳのパーティションにおける保護を実現している。

【００４２】

以上、詳述したように、これらの実施の形態によれば、ＰＡＲＴＩＥＳパーティションにおける書き込み制限を実現し、通常のアプリケーションをＰＡＲＴＩＥＳパーティション用のアプリケージョンとして使用することができる。このとき、ＰＡＲＴＩＥＳパーティション用にアプリケーションを変更し、開発する必要はない。即ち、ＰＡＲＴＩＥＳパーティション上のアプリケーション側で問題を解消しなくとも、書き込み制限を行うことが可能となる。また、予期しない書き込みに対する対応が不要となり、更に、ＰＡＲＴＩＥＳの仕様の利用範囲を拡張することが可能となる。

【００４３】

【発明の効果】

このように、本発明によれば、例えばＨＤＤ等の記憶装置において、ユーザから隠蔽された領域に格納されたアプリケーションに対する書き込み保護を実現することができる。

【図面の簡単な説明】

【図１】　実施の形態１におけるコンピュータシステムの全体構成を示した図である。

【図２】　実施の形態１における書き込み保護方法を説明するための図である。

【図３】　実施の形態１におけるＰＡＲＴＩＥＳアプリケーションのブートの流れを示したフローチャートである。

【図４】　実施の形態２におけるコンピュータシステムの全体構成を示した図である。

【図５】　実施の形態２における書き込み保護方法を説明するための図である。

【図６】　実施の形態２におけるＰＡＲＴＩＥＳアプリケーションのブートの流れを示したフローチャートである。

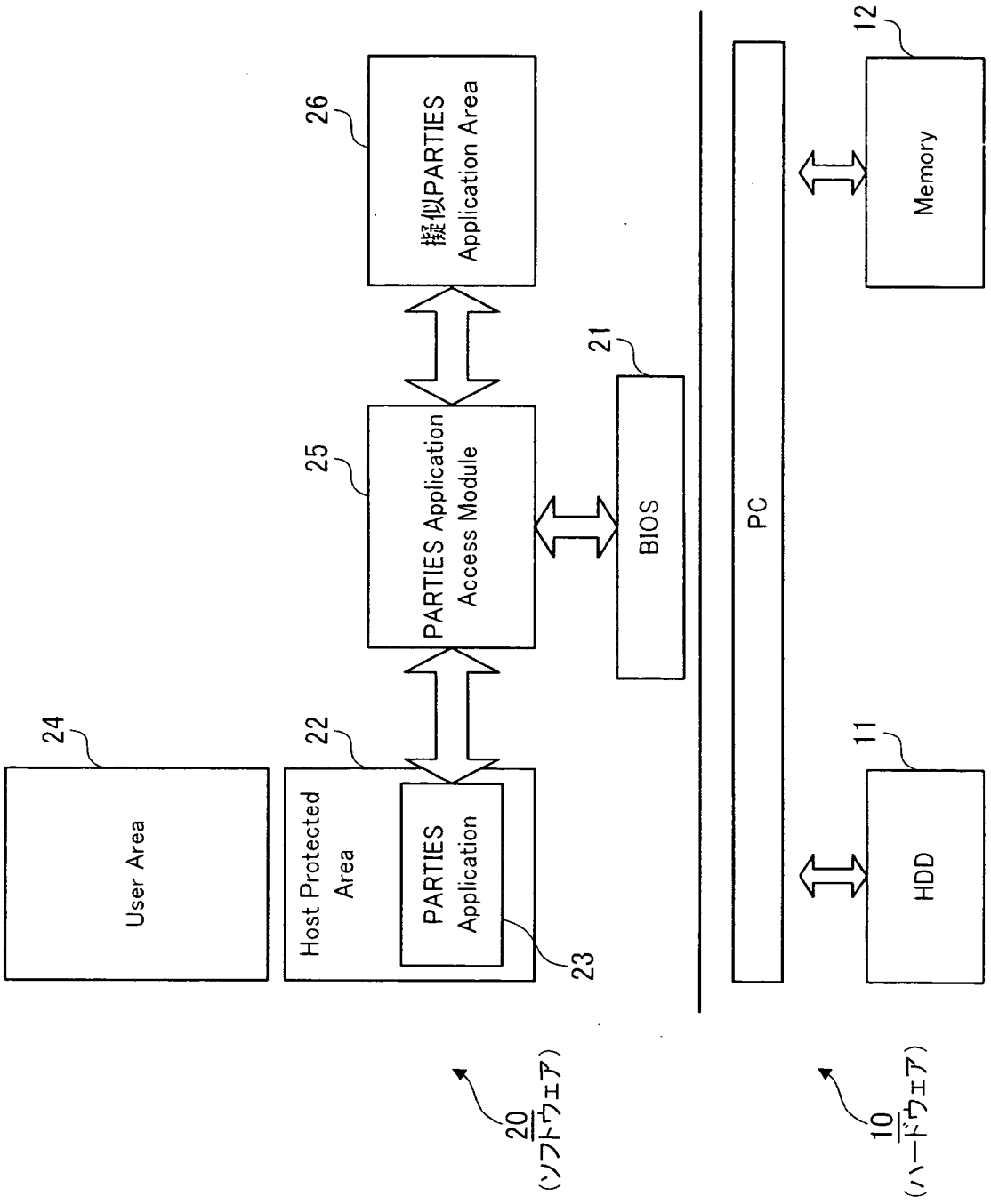
【図７】　ＨＤＤにおけるＰＡＲＴＩＥＳの機能を説明するための図である。

【符号の説明】

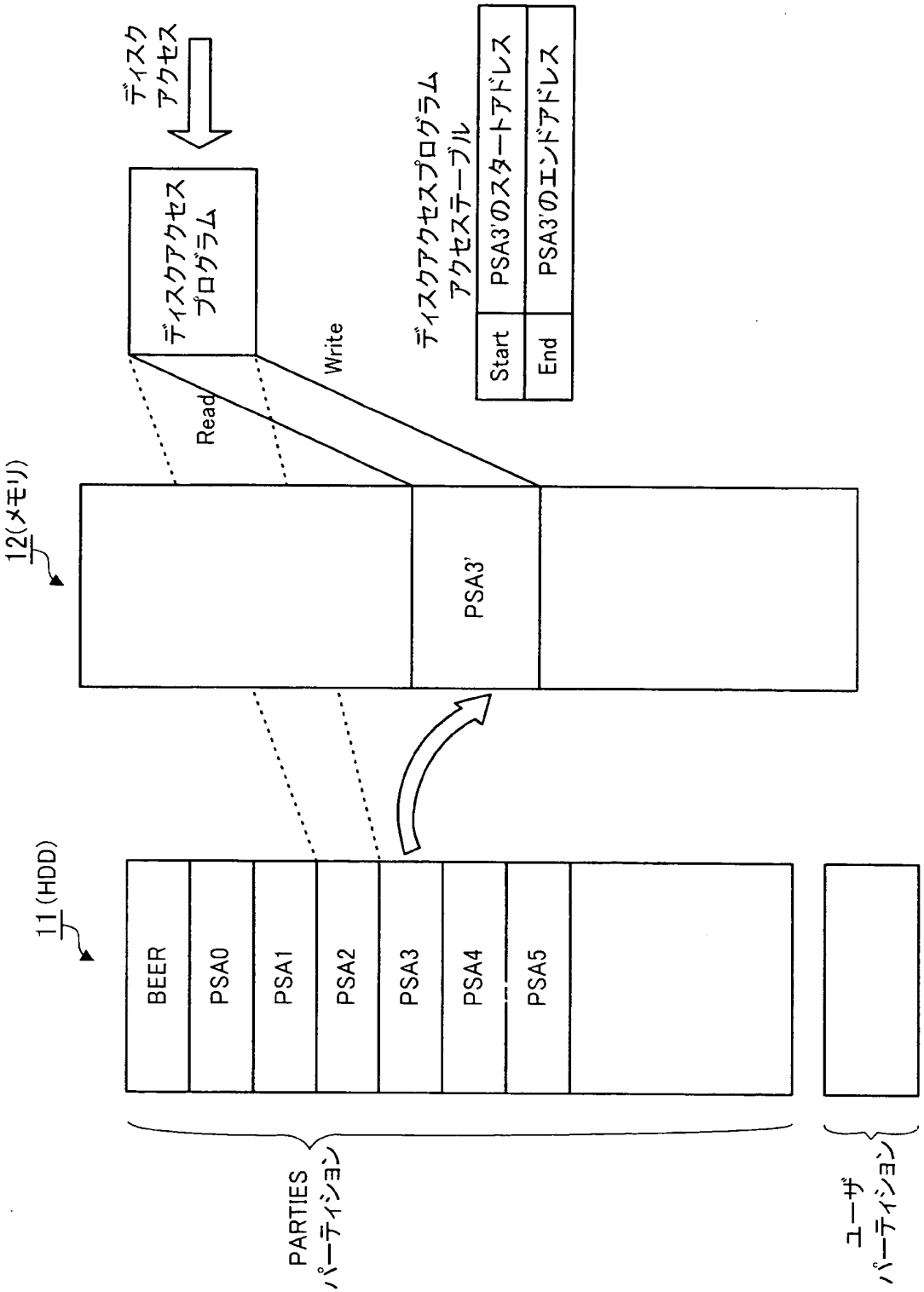
１０…ハードウェア、１１…ＨＤＤ(Hard Disk Drive)、１２…メモリ(Memory)、２０…ソフトウェア、２１…ＢＩＯＳ(Basic Input/Output System)、２２…ホストプロテクティッドエリア(Host Protected Area)、２３…ＰＡＲＴＩＥＳアプリケーション(PARTIES Application)、２４…ユーザエリア(User Area)、２５…ＰＡＲＴＩＥＳアプリケーションアクセスモジュール(PARTIES Application Access Module)、２６…擬似ＰＡＲＴＩＥＳアプリケーションエリア

【書類名】　　図面

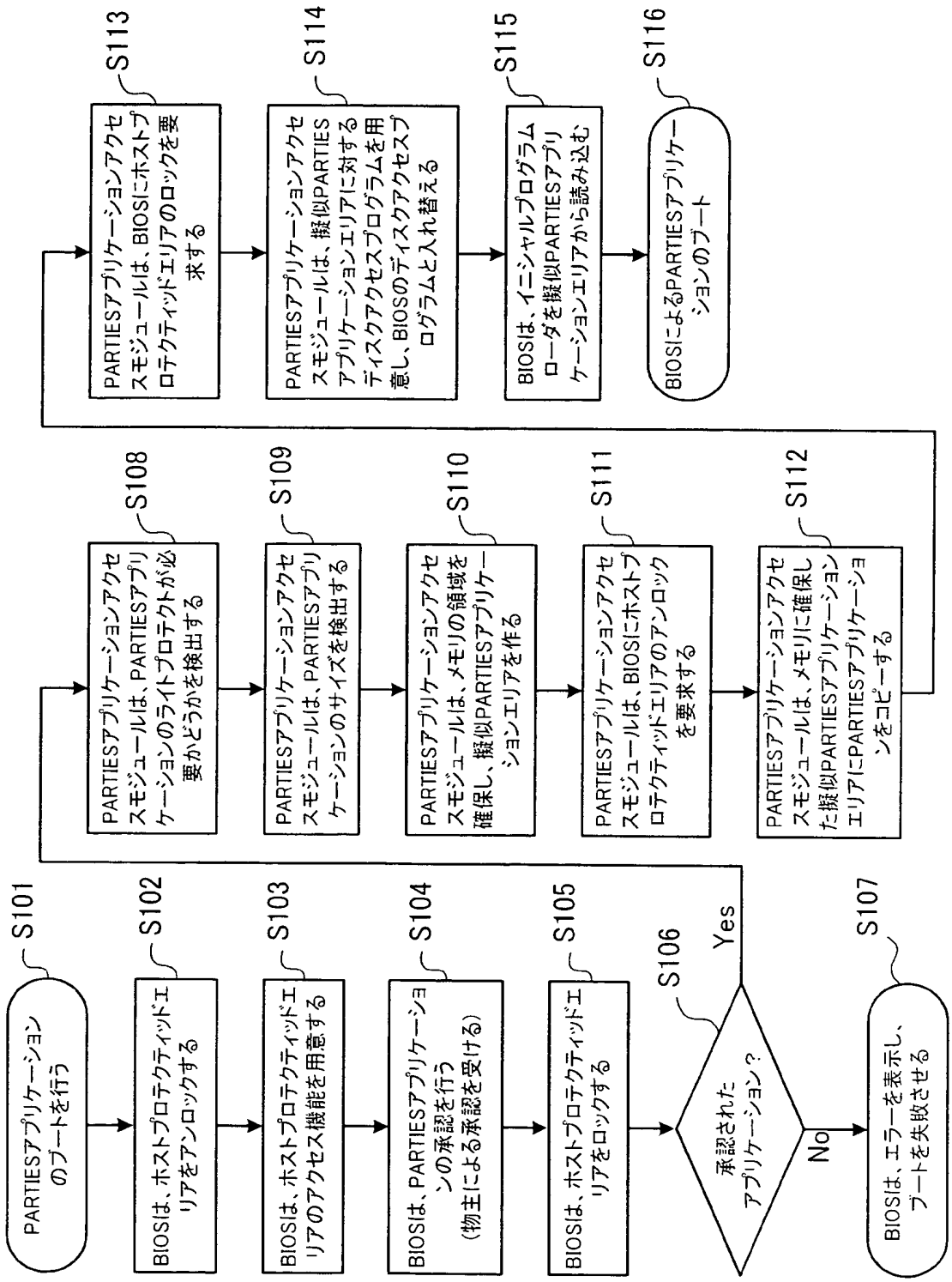
【図１】


User Area
24
Host Protected Area
22
PARTIES Application
23
PARTIES Application Access Module
25
擬似PARTIES Application Area
26
BIOS
21
PC
Memory
12
HDD
11
20 (ソフトウェア)
10 (ハードウェア)

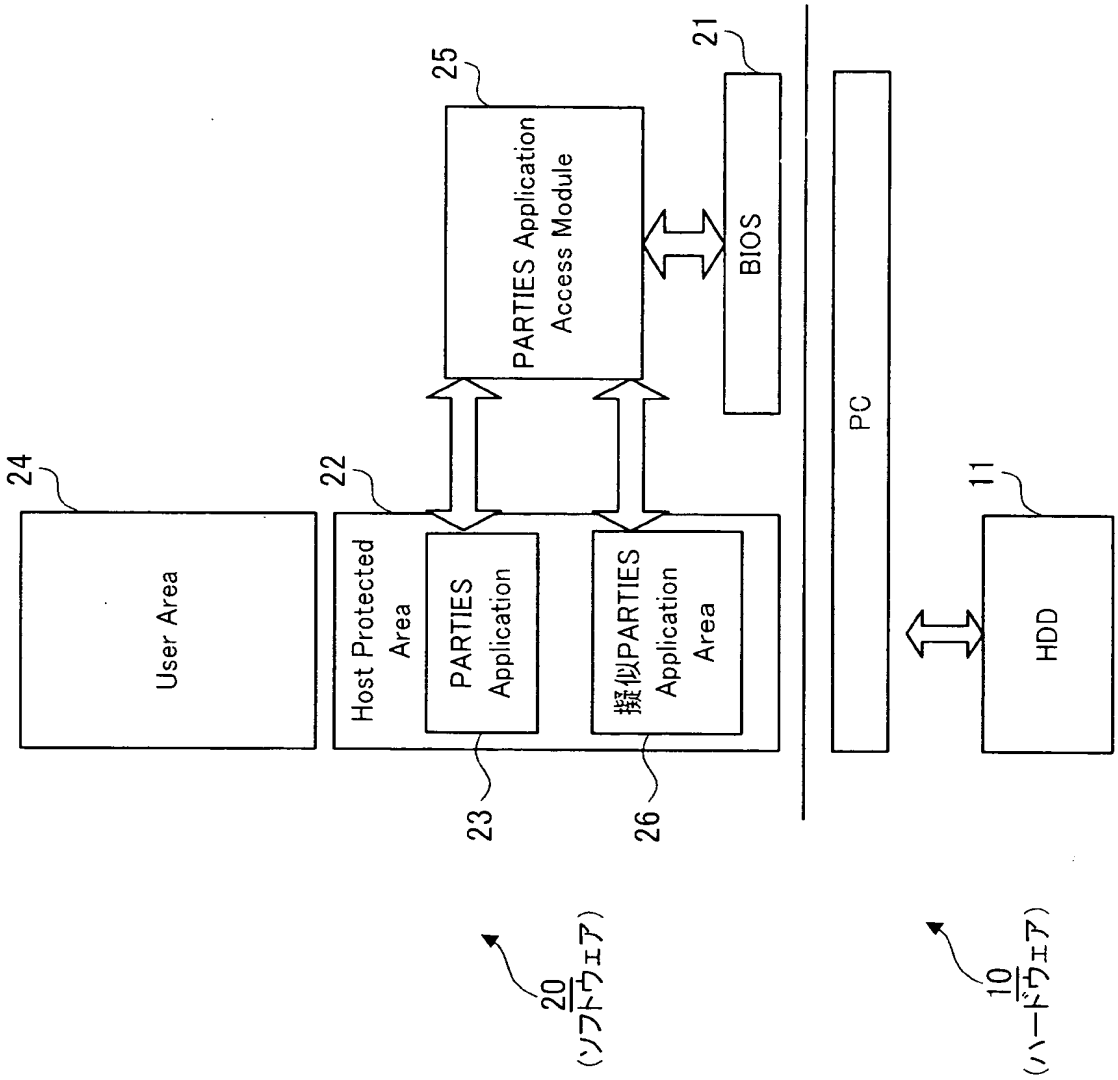
【図２】


ディスク
アクセス
ディスクアクセス
プログラム
Read
Write
ディスクアクセスプログラム
アクセステーブル
Start
End
PSA3'のスタートアドレス
PSA3'のエンドアドレス
12(メモリ)
PSA3'
11 (HDD)
BEER
PSA0
PSA1
PSA2
PSA3
PSA4
PSA5
PARTIES
パーティション
ユーザ
パーティション

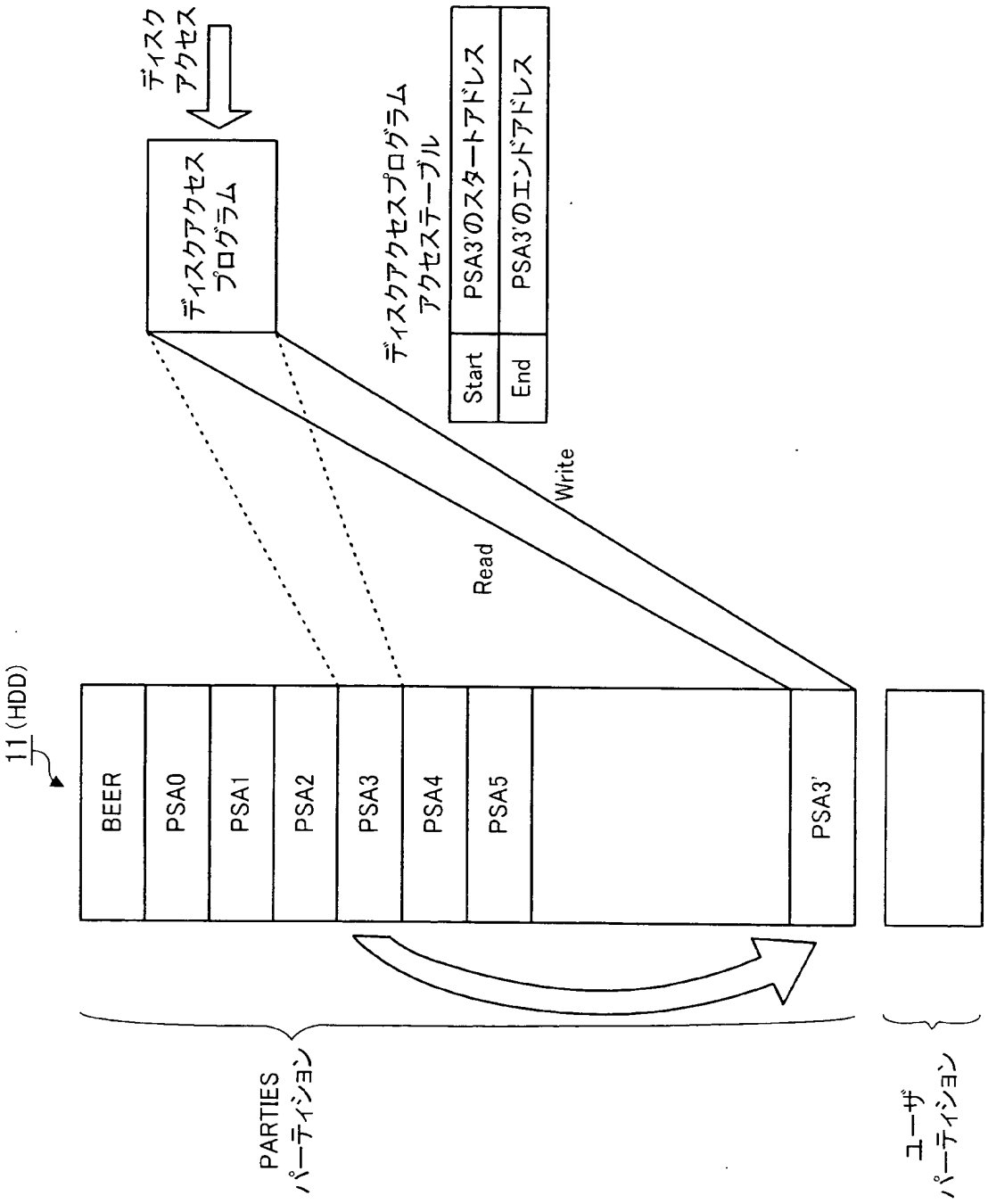
【図３】


S101
PARTIESアプリケーションのブートを行う
S102
BIOSは、ホストプロテクティッドエリアをアンロックする
S103
BIOSは、ホストプロテクティッドエリアのアクセス機能を用意する
S104
BIOSは、PARTIESアプリケーションの承認を行う（物主による承認を受ける）
S105
BIOSは、ホストプロテクティッドエリアをロックする
S106
承認されたアプリケーション？
Yes
No
S107
BIOSは、エラーを表示し、ブートを失敗させる
S108
PARTIESアプリケーションアクセスモジュールは、PARTIESアプリケーションのライトプロテクトが必要かどうかを検出する
S109
PARTIESアプリケーションアクセスモジュールは、PARTIESアプリケーションのサイズを検出する
S110
PARTIESアプリケーションアクセスモジュールは、メモリの領域を確保し、擬似PARTIESアプリケーションエリアを作る
S111
PARTIESアプリケーションアクセスモジュールは、BIOSにホストプロテクティッドエリアのアンロックを要求する
S112
PARTIESアプリケーションアクセスモジュールは、メモリに確保した擬似PARTIESアプリケーションエリアにPARTIESアプリケーションをコピーする
S113
PARTIESアプリケーションアクセスモジュールは、BIOSにホストプロテクティッドエリアのロックを要求する
S114
PARTIESアプリケーションアクセスモジュールは、擬似PARTIESアプリケーションエリアに対するディスクアクセスプログラムを用意し、BIOSのディスクアクセスプログラムと入れ替える
S115
BIOSは、イニシャルプログラムローダを擬似PARTIESアプリケーションエリアから読み込む
S116
BIOSによるPARTIESアプリケーションのブート

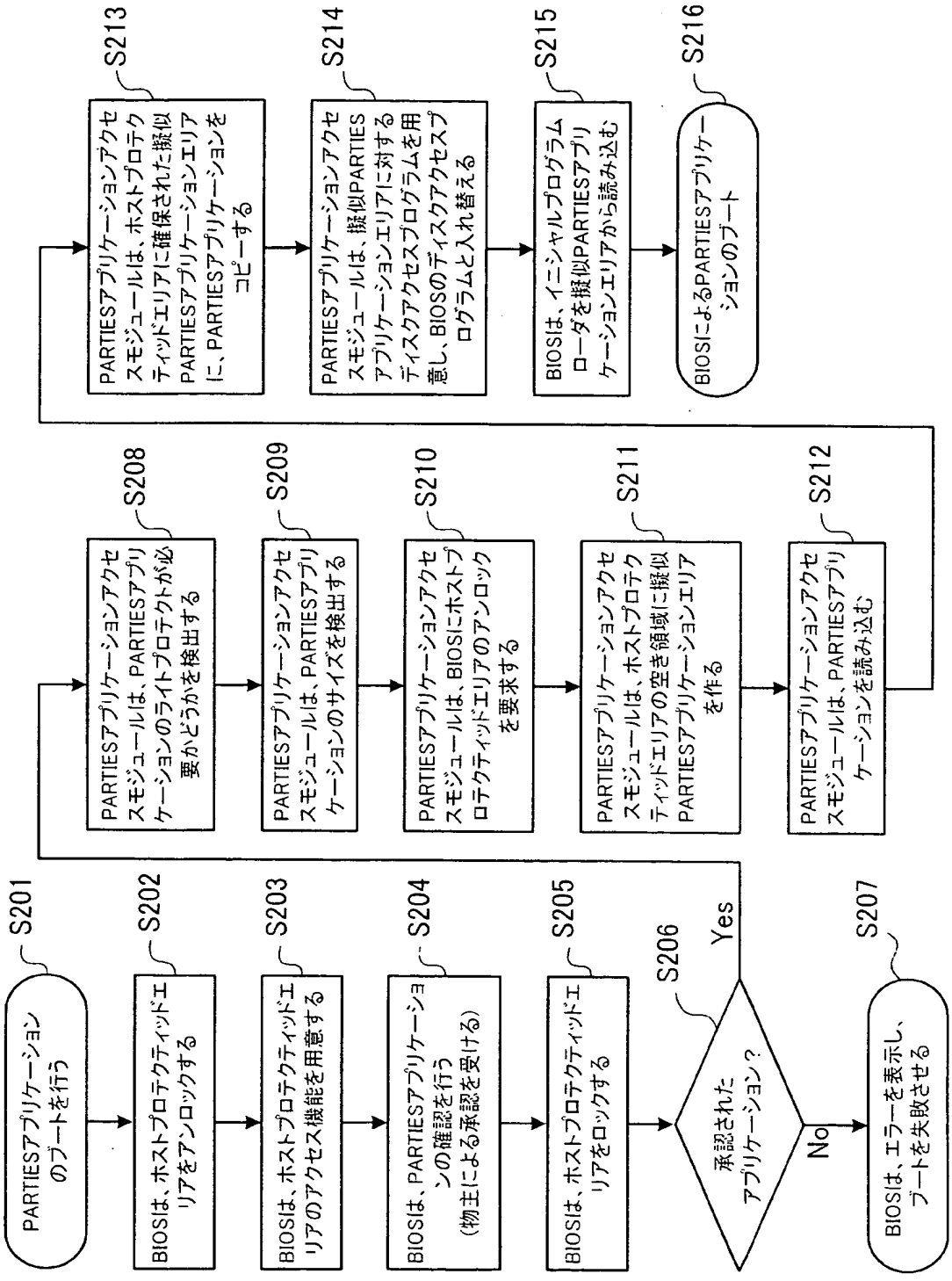
【図４】


25
PARTIES Application Access Module
21
BIOS
PC
24
User Area
22
Host Protected Area
PARTIES Application
擬似PARTIES Application Area
11
HDD
23
26
20
(ソフトウェア)
10
(ハードウェア)

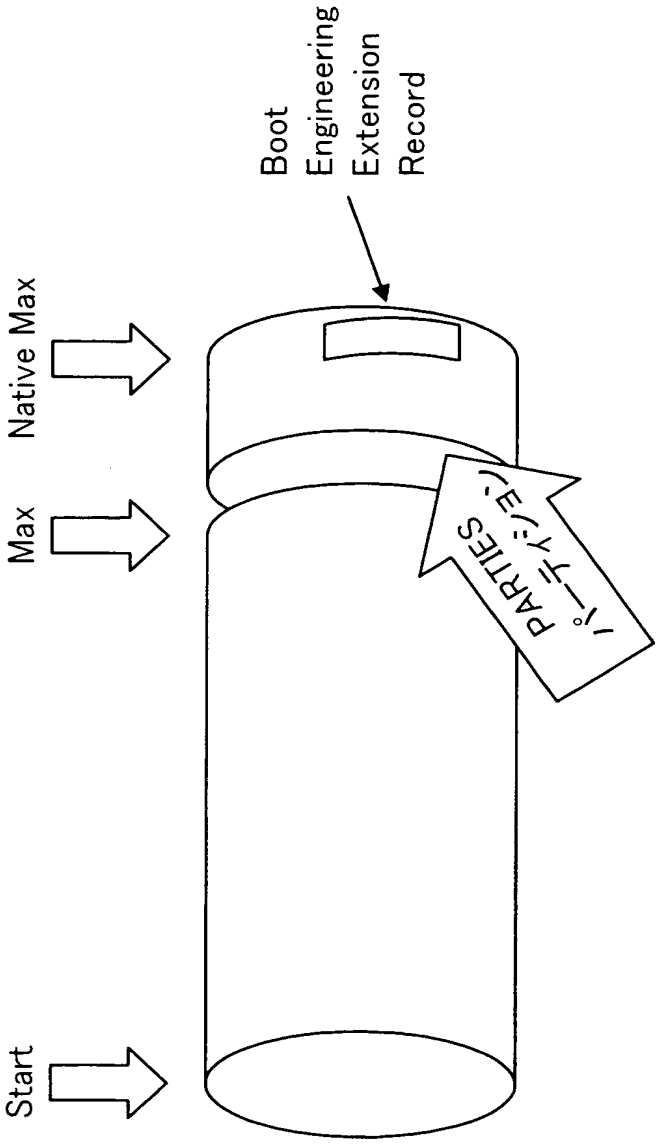
【図５】


ディスク
アクセス
ディスクアクセス
プログラム
ディスクアクセスプログラム
アクセステーブル
Start
End
PSA3'のスタートアドレス
PSA3'のエンドアドレス
Write
Read
11 (HDD)
BEER
PSA0
PSA1
PSA2
PSA3
PSA4
PSA5
PSA3'
PARTIES
パーティション
ユーザ
パーティション

【図６】


S201
PARTIESアプリケーション のブートを行う
S202
BIOSは、ホストプロテクティッドエリアをアンロックする
S203
BIOSは、ホストプロテクティッドエリアのアクセス機能を用意する
S204
BIOSは、PARTIESアプリケーションの確認を行う (物主による承認を受ける)
S205
BIOSは、ホストプロテクティッドエリアをロックする
S206
承認されたアプリケーション？
Yes
No
S207
BIOSは、エラーを表示し、ブートを失敗させる
S208
PARTIESアプリケーションアクセスモジュールは、PARTIESアプリケーションのライトプロテクトが必要かどうかを検出する
S209
PARTIESアプリケーションアクセスモジュールは、PARTIESアプリケーションのサイズを検出する
S210
PARTIESアプリケーションアクセスモジュールは、BIOSにホストプロテクティッドエリアのアンロックを要求する
S211
PARTIESアプリケーションアクセスモジュールは、ホストプロテクティッドエリアの空き領域に擬似PARTIESアプリケーションエリアを作る
S212
PARTIESアプリケーションアクセスモジュールは、PARTIESアプリケーションを読み込む
S213
PARTIESアプリケーションアクセスモジュールは、ホストプロテクティッドエリアに確保された擬似PARTIESアプリケーションエリアに、PARTIESアプリケーションをコピーする
S214
PARTIESアプリケーションアクセスモジュールは、擬似PARTIESアプリケーションエリアに対するディスクアクセスプログラムを用意し、BIOSのディスクアクセスプログラムと入れ替える
S215
BIOSは、イニシャルプログラムローダを擬似PARTIESアプリケーションエリアから読み込む
S216
BIOSによるPARTIESアプリケーションのブート

【図７】


Boot
Engineering
Extension
Record
Native Max
Max
Start
PARTIES
パーティション

【書類名】　　要約書

【要約】

【課題】　ＨＤＤ等の記憶装置において、ユーザから隠蔽された領域に格納されたアプリケーションに対する書き込み保護を実現する。

【解決手段】　ユーザの環境で動作するエリアであるユーザエリア２４と、ユーザから保護されたエリアであるホストプロテクティッドエリア２２とに区別されてデータを保持するＨＤＤ１１に対し、ホストプロテクティッドエリア２２からのブートをサポートすると共にこのホストプロテクティッドエリア２２にあるＰＡＲＴＩＥＳアプリケーション２３に対する物主証明のための承認をサポートするＢＩＯＳ２１と、ＰＡＲＴＩＥＳアプリケーション２３をメモリ１２の空き領域にコピーして擬似ＰＡＲＴＩＥＳアプリケーションエリア２６を生成するＰＡＲＴＩＥＳアプリケーションアクセスモジュール２５とを備えた。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００３－０１８３０９
受付番号	５０３００１２９７６４
書類名	特許願
担当官	土井　恵子　　４２６４
作成日	平成１５年　３月１０日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　390009531

【住所又は居所】　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100108501

【住所又は居所】　神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社　知的所有権

【氏名又は名称】　上野　剛史

【復代理人】　申請人

【識別番号】　100104880

【住所又は居所】　東京都港区赤坂５－４－１１　山口建設第２ビル６Ｆ　セリオ国際特許事務所

【氏名又は名称】　古部　次郎

【選任した復代理人】

【識別番号】　100118201

次頁有

認定・付加情報（続き）

【住所又は居所】　東京都港区赤坂５－４－１１　山口建設第二ビル
６Ｆ　セリオ国際特許事務所
【氏名又は名称】　千田　武

次頁無

特願２００３－０１８３０９

出　願　人　履　歴　情　報

識別番号　　［３９０００９５３１］

１．変更年月日　　２０００年　５月１６日
［変更理由］　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション

２．変更年月日　　２００２年　６月　３日
［変更理由］　住所変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション